

EMAIL SECURITY

THE GOOD THE BAD & THE UGLY

THE GOOD – ORGANISATIONS CAUGHT IN THE NET

- 1** Phishing up 600% in 2020
- 2** 92% of malware is delivered by email
- 3** 5.9 million Ransomware attacks in the UK
- Education #1** Target for Ransomware
- 150,000+** systems in UK Healthcare sector still running Windows 7
- 54%** of Universities reported a data breach in 2020

EXPLOSION OF MALICIOUS MICROSOFT OFFICE FILES

UP by 176% in 2020 Approx **70,184** incidents in total including a new Excel malware variant

THE LOW DOWN - WHO HAS BEEN AFFECTED

- 56% CRITICAL INFRASTRUCTURE**
56% of utilities lost operational data due to cyber attack (Siemens/Ponemon)
- 24% EDUCATION**
24% rise in cyber attacks in September '20 alone (Education Technology)
- 60% PUBLIC SECTOR**
60% of Companies targeted (UK Gov)
- 100% PROFESSIONAL SERVICES**
100% of UK law firms suffered a security event in 2020 (PWC Annual Law Firm Survey)

THE BAD - THE HACKING TRUTH

The most impersonated brands so far in 2021

"A national cyber emergency is a probability"
Director of Government NCSC

THE SOCIAL ENGINEERING FACTOR

YOU may not be the main target yet, **BUT** just be part of a much bigger **SCAM** that could affect you down the line

HACKERS MASQUERADE AS...

- Companies/people you do business with
- Internal departments
- Trusted brands
- Friends and family

HOW IT HITS YOUR POCKET

AVERAGE cost of CYBERATTACKS to UK BUSINESSES

Malware	£1.57M
Web Based Attacks	£1.52M
DoS Attacks	£1.31M
Malicious Insiders	£0.96M
Malicious Code	£0.96M
Phishing & Social Engineering	£0.96M
Ransomware	£0.52M
Botnets	£0.26M

AVERAGE TIME to resolution of CYBERATTACKS to UK BUSINESSES

Malware	6.4 days
Web Based Attacks	22.4 days
DoS Attacks	16.8 days
Malicious Insiders	50 days
Malicious Code	55.2 days
Phishing & Social Engineering	20 days
Ransomware	23.1 days
Botnets	2.5 days

Source: IT Governance

THE COST OF AN ATTACK

Aside from reputational damage and any ransom demands

INFORMATION TECHNOLOGY COSTS
Restoring compromised systems

INFORMATION TECHNOLOGY COSTS
Responding to customer concerns in the aftermath of a breach is critical to retention, but an increase in call/support centre activity can add hundreds of hours of work.

OPERATIONAL DISRUPTION COSTS
Suspending IT and other critical services is a common response to a breach

OPERATIONAL DISRUPTION COSTS
Forensics teams pursuing legal action against cyber criminals combined with defending the business from damages resulting from a breach

GDPR supervisory authorities issued £2.6 million in fines in Q2 2020

THE UGLY - NOT ALL BAD NEWS

A reported overall **DECREASE** in spend recovering from security incidents compared with 2019

BECAUSE organisations have responded to the need for **investment**

BUT

Not all email security platforms are created equal and as **MALWARE** is the costliest form of attack, check where yours sits in our **PRICE vs FEATURE** set table

Please get in touch if you think you could be doing better

- 1 ARE YOU STILL VULNERABLE?**
The easy way to find out what will get through in the event of a phishing attack so you can do something about it before it happens!
[TAKE THE TEST](https://emailsecuritytester.com)
- 2 OR ARE YOU PAYING TOO MUCH?**
You could **save up to 30 - 50%** with identical feature sets to you existing Email Security provider
[TAKE THE CHALLENGE](https://www.myredfort.com/articles/email-security/ta-ke-the-renewal-challenge)

/LIBRAESVA

theamigosnetwork

© Copyright 2021